IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

| | |
|---|---|
| UNITED STATES OF AMERICA<br>v.<br>CONOR BRIAN FITZPATRICK,<br>a/k/a "Pompompurin"<br>Defendant. | Case No. 1:23-CR-119<br>Hon. Leonie M. Brinkema<br>Sentencing: September 16, 2025 |

**POSITION OF THE UNITED STATES WITH RESPECT TO RESENTENCING**

Defendant Conor Brian Fitzpatrick was the founder and lead administrator of BreachForums, the largest English-language data breach site of its kind. The defendant designed BreachForums as a cybercrime forum dedicated to furnishing the cyber underworld with access to customer and user databases that hackers stole from victim companies, organizations, and governmental entities. These databases often contained the sensitive personally identifying information (PII) of millions of Americans. At its height, BreachForums boasted almost one thousand data sets, comprised of billions of individual records, and more than 300,000 members.

The defendant created BreachForums in March 2022, almost immediately after Raidforums, the prior leading English-language data breach forum, was disrupted by the FBI and its leader publicly arrested in early 2022. The defendant and his co-conspirators earned nearly $700,000 through the operation of BreachForums. The defendant's crimes left numerous victims, many of whom suffered substantial monetary and reputational losses, and in the case of one victim company, the suicide death of its CEO. The defendant also downloaded and stored child

pornography, including videos of prepubescent girls masturbating. In doing so, he perpetuated yet another set of victims.

The defendant now comes before the Court for resentencing after having pleaded guilty to conspiracy to commit access device fraud, in violation of 18 U.S.C. §§ 1029(b)(2) and 3559(g)(1); solicitation for the purpose of offering access devices, in violation of 18 U.S.C., §§ 1029(a)(6) and 2; and possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B) and (b)(2). The applicable Guidelines range was correctly calculated in the Presentence Investigation Report ("PSR") as 120 months' imprisonment as to Counts 1 and 2 and 188 months to 235 months' imprisonment as to Count 3. *See* Dkt. 63 (PSR) ¶ 122.

For the reasons below, the United States respectfully recommends that the Court impose a sentence of 188 months' imprisonment, which is sufficient, but not greater than necessary, to reflect the seriousness of the crime, the significant harm caused by the defendant's crimes, the risk of recidivism, and to deter the defendant and others who may seek to profit from this type of widespread cybercrime in the future. In support of its recommendation, the government incorporates its Position with Respect to Sentencing (Dkt. 65), the exhibits attached thereto, as well as the information below.

**BACKGROUND**

From at least in or around October 2020 through 2022, the defendant used the online moniker "Pompompurin" to make posts on Raidforums offering to sell valuable breached

databases.[1] PSR ¶ 25. Then, starting in or around March 2022, the defendant leveraged the reputation he built on Raidforums to create and administer BreachForums with the assistance of co-conspirators, including an evolving staff of moderators. *Id.* ¶¶ 18, 26. The defendant and his co-conspirators gained at least $698,714 through the operation of BreachForums. *Id.* ¶ 39.

## I. Defendant's Creation and Operation of BreachForums

In March 2022, the defendant founded and became the lead administrator of BreachForums. PSR ¶ 36. The defendant also hired and managed a staff of moderators (i.e., co-conspirators) who played an important role in ensuring that BreachForums operated properly and who performed traditional administrative activity, such as transmitting messages to warn members of conduct that violated BreachForums' rules. *Id.* ¶ 38.

As the name "BreachForums" suggests, the purpose of BreachForums, and the defendant's intent in operating the forum, was to traffic, and aid and abet others in trafficking, breached or stolen databases containing access devices, among other things. PSR ¶ 27. In particular, the defendant intentionally ran BreachForums in a manner that made it an attractive marketplace for cybercriminals to frequent in an effort to buy, sell, or trade stolen or hacked access devices. *Id.*

To achieve these objectives, the defendant took a leading role in all aspects of BreachForums' operations. PSR ¶ 36. Among other things, he (i) designed and administered the

[1] In the modern digital economy, large companies and organizations often collect and store a significant amount of PII about their customers or users in large online repositories known as databases. The types of data stored in customer databases can range from limited identity information, such as customer name, email address, and contact information, to far more sensitive material, such as customer login credentials for accessing online accounts and services, bank account numbers, payment card data, social security numbers, dates of birth, and driver's license information. When this sensitive personal data falls into the wrong hands through computer hacking—often termed "data breaches"—or other means, it can be easily exploited by fraudsters to conduct unauthorized financial transactions or assume the identity of unsuspecting Americans in furtherance of other financial fraud schemes.

website's software and computer infrastructure; (ii) registered domains to host or provide access to the BreachForums website in a manner that prevented the effective identification of him as the person who registered it;[2] (iii) established and enforced the website's rules; (iv) created and managed sections of the website dedicated to promoting the buying and selling of stolen data; (v) operated a middleman service; (vi) approved and uploaded breached databases to the BreachForums' "Official" network for delivering content; and (vii) provided other assistance to BreachForums members seeking to buy and sell illicit material on the website, including by investigating and sometimes vouching for the authenticity of stolen data. *Id.*

In accordance with the defendant's design, any individual with an Internet browser could access and view the BreachForums website without a membership. PSR ¶ 28. However, the website required an individual to sign up for a membership to solicit items for sale or to purchase items. *Id.* BreachForums offered tiers of membership options that cost varying amounts of money, including a "God" membership that offered almost unlimited access to the BreachForums website and features. *Id.*

The defendant further organized the BreachForums website into sections that enabled members to offer, purchase, and provide access to different categories of hacked or stolen data and other contraband. PSR ¶ 26. In a "Marketplace" section and "Leaks Market" subsection, for example, BreachForums members bought and sold hacked or stolen databases, tools for committing cybercrime, and other illicit material. *Id.* ¶ 29. Items commonly sold in this section included bank account information, social security numbers, other PII, and login information for compromised online accounts, such as usernames and passwords to access accounts with service

[2] Some of the domains registered by the defendant included breached.vc, breached.to, breachedforums.com, breachforums.net, and breachforums.org.

providers and merchants. *Id.* BreachForums also supported additional sections in which users posted stolen data and discussed tools and techniques for hacking and exploiting that information, including in the "Cracking," "Leaks," and "Tutorials" sections. *Id.* ¶ 31. Examples of stolen data offered or trafficked in these sections include:

- On December 18, 2022, a BreachForums user with the moniker "USDoD" posted details of approximately 87,760 members of InfraGard, a partnership between the Federal Bureau of Investigation (FBI) and private sector companies focused on the protection of critical infrastructure. PSR ¶ 30.

- On January 4, 2023, information obtained from a major U.S.-based social networking site was posted by a user with the moniker "StayMad." PSR ¶ 30. This information included names and contact information for approximately 200 million users. *Id.*

- On January 21, 2023, a BreachForums user with the moniker "Sin" published a post advertising a list of approximately 20 million user records for a company that controls two U.S.-based background check services ("Victim-1"). PSR at p. 39-40 (Declaration of Victim-1). Victim-1 reports that the breached database contained the PII of user accounts created between 2011 and April 2019, including subscriber name, email address, sparse phone number, password reset token and hashed password. *Id.*

- On March 9, 2023, a BreachForums user with the moniker "denfur" also posted a message revealing the PII of tens of thousands of U.S. citizens. PSR ¶ 30. The message included a link to download a file containing names, dates of birth, social security numbers, employment information, and health insurance information stolen from a health insurance exchange. *Id.*

To facilitate transactions among BreachForums members operating in these sections, the defendant offered a "middleman" service in which he acted as a trusted middleman, or escrow, between individuals on the website who sought to buy and sell information. PSR ¶ 32. The defendant's middleman service substantially facilitated and encouraged the dissemination of hacked or stolen data through BreachForums because it enabled purchasers and sellers to verify the means of payment and contraband files being sold prior to executing the purchase and sale. *Id.* The defendant's standardized middleman process required members to notify him of the "product"

they sought to trade. *Id.* In a post announcing the service, the defendant boasted that he had already facilitated over $430,000 in transactions as a middleman with "zero issues" as of November 6, 2022—*i.e.*, the midpoint of the scheme. *Id.* ¶ 45. Examples of the transactions for which the defendant served as a trusted middleman include:

- In July 2022, the defendant served as the middleman for a transaction in which an FBI online covert employee ("OCE") in the Eastern District of Virginia paid a BreachForums user, expo2020, approximately $5,000 to purchase the PII and bank account information of approximately 15 million U.S. persons. PSR ¶¶ 46-47. The defendant facilitated the transaction despite receiving notice that expo2020 was offering "USA FULLZ. Name.ssn.dob.address.dl," and the data included birth dates, social security numbers, and bank account information for use in conducting financial scams. *Id.*

- Likewise, in August 2022, the defendant served as the middleman for a transaction in which an OCE paid a BreachForums user, jigsaw, to buy unauthorized access to the accounting system of a U.S. healthcare company ("Victim-2"), and sample files from the network containing driver's license photos, insurance cards, and partial credit card information for approximately 13 individuals. PSR ¶¶ 48-52. As with the prior purchase, the defendant completed the transaction after being notified that the buyer intended to use the unauthorized access to make money. *Id.* ¶ 51.

BreachForums also managed a section titled "Official," which the defendant described as a "[f]orum where databases stored on our own servers are kept." PSR ¶ 33. As of March 7, 2023, approximately 888 databases containing over 14 billion individual records were available for purchase on BreachForums' Official "content distribution network" (CDN) through a "credits" system that the website administered. *Id.* ¶¶ 33-34. Credits were available for purchase on the website or earned through contributing content. *Id.* BreachForums members seeking to post databases to the Official BreachForums CDN were required to contact the defendant directly, who would then only upload those databases that he approved. *Id.*

For instance, on May 8, 2022, the defendant approved the addition to BreachForums' Official CDN of a customer database from a U.S.-based internet hosting and security services company that purported to contain the names, addresses, phone numbers, usernames, password

hashes, and email addresses for approximately 8,000 customers, as well as payment card information for approximately 1,900 customers. PSR ¶ 42. The approval caused the database to be offered for sale through forum credits to BreachForums members on the Internet, including an OCE who viewed the solicitation. *Id.* On October 27, 2022, the FBI OCE purchased and downloaded this database for 8 credits[3] and confirmed that the database contained apparently stolen customer PII, such as usernames, password hashes, credit card numbers, expiration dates, and card verification values. *Id.* ¶¶ 43-44.

The defendant also knowingly and intentionally provided advice and other support that aided the illicit activities of BreachForums members. PSR ¶¶ 53-55. For instance, in September 2022, the defendant provided a BreachForums member with a roadmap for how to monetize a breached e-commerce database that included approximately 16 million records. *Id.* ¶ 55. In relevant part, the defendant advised the user to first try to extort the victim company for money, and then try to sell the database to others if the victim refused to pay. *Id.* ("I[']d try getting money out of them first, and if they refuse try selling it."). The defendant then explained that he would value the database at about "a few thousand" after the user sought pricing guidance. *Id.*

In addition, the defendant sometimes assured his members that he would help them obfuscate their identities from law enforcement. PSR ¶¶ 53-54. For instance, on May 11, 2022, the defendant sent a private message through BreachForums in which he agreed to delete the registration Internet Protocol (IP) address of a BreachForums member who wanted it deleted "for privacy reasons, I don't want cops randomly scouting it for dumb shit I do." *Id.* ¶ 53. Similarly, on May 24, 2022, the defendant sent a private message to a BreachForums member in which he

[3] As of October 20, 2022, credits cost approximately $0.25 each, and were available in bundles of 30, 60, 120, 240, and 500. Various forms of cryptocurrency were accepted as payment.

promised to provide "falsified [registration] information" if law enforcement asked. *Id.* ¶ 54. As part of the reply, the defendant noted "[s]ure, although I doubt law enforcement would even bother making legal requests to a hacking forum lmao." *Id*.

## II. Fitzpatrick's Knowing Possession of Child Pornography

The defendant knowingly possessed approximately 26 digital files depicting minors engaged in sexually explicit conduct. PSR ¶ 56. The defendant saved these files in two folders on his Samsung solid state drive ("Samsung SSD"). *Id.* ¶¶ 56-57. These files included, for example, a video file with 13y-fully-nude in the title, which depicted a minor female who exposed her genitals to the camera and masturbated. *Id.* ¶ 59. The defendant saved this file to his Samsung SSD on February 9, 2023, and later opened it. *Id*. Another video file in the defendant's collection depicted two prepubescent girls who exposed their genitals to the camera and masturbated. *Id.* ¶ 60. The defendant also saved this file to his Samsung SSD on February 9, 2023, and later opened the file after he saved it. *Id*.

## III. Procedural History and Pretrial Violation

On March 15, 2023, the defendant was arrested pursuant to a criminal complaint and arrest warrant, which charged him with conspiracy to commit access device fraud, in violation of 18 U.S.C. § 1029(b)(2). Dkt. 1. The defendant made his initial appearance in the Southern District of New York, where he was released on a personal recognizance bond and ordered to comply with pretrial supervision and various other terms and conditions of release. *See* Dkt. 10. On March 24, 2023, the defendant made his initial appearance in the Eastern District of Virginia and was ordered to not access VPN software as an additional condition of release. *See* Dkt. 16.

On July 13, 2023, the defendant pleaded guilty to a three-count Information that charged him with conspiracy to commit access device fraud, in violation of 18 U.S.C. §§ 1029(b)(2) and

3559(g)(1) (Count 1); solicitation for the purpose of offering access devices, in violation of 18 U.S.C. §§ 1029(a)(6) and 2 (Count 2); and possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B) and (b)(2) (Count 3). *See* Dkt. 40 (Plea Agreement).

The Honorable T.S. Ellis, III permitted the defendant to remain on bond pending sentencing but imposed certain additional terms and conditions to the existing bond conditions ordered in March 2023. *See* Dkt. 44. Notably, the defendant was ordered to not access a computer and/or the Internet without computer monitoring software installed by pretrial services and not use any tools for obfuscating his identity, such as virtual private networks (VPNs). *See id.*

On December 21, 2023, Judge Ellis authorized an arrest warrant for the defendant based on a Petition submitted by the U.S. Probation Office (USPO) detailing the defendant's alleged violation of his conditions of release. *See* Dkt. 54. Details concerning the USPO petition and other relevant facts are set forth in Exhibits A and B (Dkts. 65-1 and 65-2) to the United States' Position with Respect to Sentencing (Dkt. 65). On January 2, 2024, the defendant was arrested on the pretrial violation and detained pending his sentencing hearing on January 19, 2024.

At the sentencing hearing on January 19, 2024, the defendant conceded the pretrial violation but argued that the conduct, namely statements he made on the unmonitored device, was in "bad jest" was "not criminal in and of itself" and could be attributed, at least in part, to his purported lack of treatment at that time. *See* Dkt. 77 (Transcript of Sentencing Hearing) at 14-15. The Court sentenced the defendant to time served (17 days), followed by a period of 20 years of supervised release. Dkt. 73 (Judgment). The Court expressed concern that the Bureau of Prisons (BOP) would not be able to treat the defendant's autism spectrum disorder (ASD) and that he would be victimized in prison. Dkt. 77 at 24. The government appealed the Court's sentence, and

the Fourth Circuit vacated and remanded for resentencing. *See U.S. v. Fitzpatrick*, 126 F.4th 348 (4th Cir. 2025). A resentencing hearing is scheduled for September 16, 2025.

## SENTENCING ANALYSIS

### I. Statutory Penalties and Sentencing Guidelines Calculations

Counts 1 and 2 of the Information each carry a maximum sentence of 10 years' imprisonment and a term of supervised release up to 3 years. *See* 18 U.S.C. §§ 1029(a)(6) and (b) and 3853(b). The offense of possession of child pornography carries a maximum sentence of 20 years' imprisonment and a minimum term of supervised release of at least 5 years up to a lifetime term. *See* 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) and 3583(k).

The U.S. Probation Office correctly calculated the defendant's Guidelines as follows:

**Count Group 1: Conspiracy to Commit Access Device Fraud and Solicitation for the Purpose of Offering Access Devices**

| Guideline | Offense Level |
|---|---|
| Base offense level (USSG. § 2B1.1(a)(2)) | 6 |
| Loss amount was more than $550,000 but less than $1,500,000 (USSG § 2B1.1(b)(1)(H)) | +14 |
| Offense involved 10 or more victims (USSG § 2B1.1(b)(2)(A)(i)) | +2 |
| Offense involved receiving stolen property, and the defendant was in the business of receiving and selling stolen property (USSG § 2B1.1(b)(4)) | +2 |
| Offense involved sophisticated means and the defendant intentionally engaged in or caused the conduct constituting sophisticated means (USSG §2B1.1(b)(10)(C)) | +2 |
| Offense involved production or trafficking of any unauthorized access device or counterfeit access device (USSG § 2B1.1(b)(11)(B)(i)) | +2 |
| Offense involved the unauthorized public dissemination of personal information (USSG § 2B1.1(b)(18)(B)) | +2 |
| Defendant was an organizer or leader of a criminal activity that involved five or more participants or was otherwise extensive (USSG § 3B1.1(a)) | +4 |
| Statutory enhancement under U.S.C. § 3559(g)(1) applies (USSG § 3C1.4) | +2 |

| | |
|---|---|
| **ADJUSTED OFFENSE LEVEL** | **36** |

PSR ¶¶ 69-81.

The PSR also properly calculated an adjusted offense level of 27 for Count 3 as follows:

**Count 3: Possession of Child Pornography**

| Guideline | Offense Level |
|---|---|
| Base offense level for a violation of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (USSG § 2G2.2(a)(1)) | 18 |
| The material involved a prepubescent minor or a minor who had not attained the age of 12 years. (USSG § 2G2.2(b)(2)) | +2 |
| The offense involved the user of a computer or interactive service for the possession, transmission, receipt, or distribution of the material, or for accessing with intent to view the material. (USSG § 2G2.2(b)(6)) | +2 |
| The offense involved at least 600 images. (USSG § 2G2.2(b)(7)(D)) | +5 |
| **ADJUSTED OFFENSE LEVEL** | **27** |

PSR ¶¶ 82-89.

In the final PSR, the defendant was not awarded a two-level decrease for acceptance of responsibility under USSG § 3E1.1(a), a decision that the government supports for the reasons set forth in Exhibit A to its Position with Respect to Sentencing (Dkt. 65-1). Accordingly, as explained in the PSR, the defendant's combined adjusted offense level of 36 and criminal history category of I results in a Guidelines range of 188 months to 235 months' imprisonment. PSR ¶ 122. Because Counts 1 and 2 have a statutory maximum sentence of 10 years, the Guidelines for those counts are 120 months' imprisonment. *Id*.

As stated above, the defendant conceded that he violated the terms of his pretrial release but objected to not being awarded a two-level decrease for acceptance of responsibility. *See* Dkt. 69 at 25-28. Considering the defendant's pretrial violations, the defendant's objection should be overruled. "A defendant who enters a guilty plea is not entitled to an adjustment under this section

as a matter of right." USSG § 3E1.1, comment. (n. 3). The decrease applies only "if the defendant *clearly* demonstrates acceptance of responsibility for his offense." USSG § 3E1.1. While entry of a guilty plea prior to commencement of trial may constitute "significant evidence of acceptance of responsibility . . . this evidence may be outweighed by conduct of the defendant that is inconsistent with such acceptance of responsibility. " *Id.*, comment. (n. 3).

Here, the defendant used the Internet to commit his crimes–namely, the creation of an online platform to facilitate the distribution and sale of victim data to cybercriminals worldwide. As part of his administration of this platform, he agreed to assist criminal users of his website in concealing their true identities to avoid detection by law enforcement. After he entered his guilty pleas, the defendant used VPN services to conceal his use of the Internet and repeatedly utilized an unauthorized and unmonitored electronic device (or devices) to avoid detection by pretrial services. Even now, the defendant has not provided pretrial services or the government with this unmonitored device (or devices). Furthermore, in his unauthorized, unmonitored, chats with other individuals, the defendant expressly denied responsibility for his child pornography offense. During this time, the defendant had a Psychosexual Risk and Psychological Evaluation (Dkt. 69-3) and lied to his evaluator about his compliance with the conditions of his pretrial release. *See* Dkt. 69-3 at 9 ("Cooperation with Supervision" is "**not an area of concern** for Mr. Fitzpatrick. Per his self-report, report of his parents, and available information, Mr. Fitzpatrick has been fully compliant with the terms of his federal pretrial supervision."). While the defendant told Dr. Liebert that he was complying with the terms of his release, he was boasting to his friends online that he "[f]inally can use [his] 14 pro at home[.]" *See* Dkt. 65-2 at 4.

While the defendant did in fact plead guilty and admit to his crimes, he has not *clearly* demonstrated acceptance of responsibility since he continued to engage in evasive behavior that is

in direct violation of the orders of two different United States Judges and flatly denied culpability for one of his offenses. Therefore, the PSR correctly withheld the acceptance of responsibility credit and the defendant's objection should be denied.

## II. Sentencing Recommendation

As the Court is aware, the Guidelines are advisory, and just one factor that must be considered along with the other factors set forth in 18 U.S.C. § 3553(a).[4] Here, however, a sentence of 188 months (i.e., the low end of the Guidelines) is supported by the defendant's immense contributions to enabling widespread cybercrime, the circumstances of the offense, the risk of recidivism, and the need to adequately deter others from perpetrating similar crimes.

### A. Nature and Circumstances of the Defendant's Offenses

The known scope, breadth, and brazenness of the defendant's scheme to enable and fuel widespread cybercrime warrants a substantial period of incarceration. Indeed, as detailed above, the defendant's administration of BreachForums played an instrumental role in bringing together more than 300,000 members to solicit, distribute and access thousands of breached databases containing the stolen data of hundreds of companies, organizations, and governmental organizations of varying size and the PII of millions of U.S. persons. *See, e.g.*, PSR ¶¶ 26-52 at p. 33-42. By creating a platform for hackers and fraudsters to connect and conduct business, the defendant made it possible for BreachForums members to commit exponentially more crimes and

[4] The § 3553(a) factors include: the nature and circumstances of the offense and the history and characteristics of the defendant; the need for the sentence imposed to reflect the seriousness of the offense, to promote respect for the law, to provide just punishment for the offense, to afford adequate deterrence to criminal conduct, to protect the public from further crimes of the defendant, and to provide the defendant with needed training, medical care, or other treatment; the kinds of sentences available; the kinds of sentence and the sentencing range established for the type of offense committed; any pertinent policy statement; the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct; and the need to provide restitution to any victims of the offense.

more sophisticated crimes than any could have done alone. *See* Ben Collier et al., Cybercrime Is (Often) Boring: Maintaining the Infrastructure of Cybercrime Economies, at 1 (Cambridge Cybercrime Centre, 2020) ("It is generally accepted that the widespread availability of specialist services has helped drive the growth of cybercrime.") (hereinafter "Collier, Cybercrime Economies"), *available at* https://www.cl.cam.ac.uk/~bjc63/Crime_is_boring.pdf.

The criminal activity on BreachForums touched nearly every sector of U.S. society. As partly highlighted above, the defendant's victims included U.S.-based healthcare companies, a major public healthcare exchange, public health organizations, the FBI's InfraGard partnership for protecting critical infrastructure, major U.S.-based social media companies, U.S.-based merchants and service providers of varying size, and U.S.-based financial institutions. *See, e.g.*, PSR ¶¶ 26-52 at p. 33-41. The "Official" databases section of BreachForums alone claimed to provide access to approximately 888 stolen databases containing over 14 billion individual records. *Id.* ¶ 34.

The victim impact statements provided by victim corporations and organizations highlight some of the significant and far-reaching consequences of the defendant's crimes. Among other things, the defendant's conduct has caused victims to (i) devote time and money investigating the data breaches posted on BreachForums and tracking the dissemination of their stolen data on the dark web; (ii) face regulatory scrutiny from the Federal Trade Commission (FTC) and class action lawsuits associated with their data security practices; (iii) suffer reputational damage and business harm; and (iv) contributed to the suicide death of a victim company's CEO. *See, e.g.*, PSR at p. 33-41; *see also* Exhibit 1 (Victim Impact Statement of Victim-5) at 3.

For instance, the victim impact statement of Victim-1 described how a single post by a BreachForums member, which offered to sell a database containing the sensitive PII of 20 million users of two background check services, caused them to incur direct expenses of more than

$180,000 to investigate the data breach and track the movement of their stolen data on the dark web. *See* PSR at 40, ¶¶ 4-8. Victim-1 further detailed how the posts triggered requests from the FTC, and at least one complaint filed by an individual in the Western District of Michigan. *Id*. ¶ 7. To limit the reputational harm caused by the post, Victim-1 also spent approximately $11,492.50 on breach-related public relations.[5]

Likewise, a victim impact statement from a healthcare services company in California ("Victim-3") detailed how a BreachForums member made a post in January 2023 distributing approximately 45,523 lines of stolen data, including PII and Victim-3's source code. *See* Dkt. 65-3 (Exhibit C - Victim Impact Statement of Victim-3). The data appears to have been stolen through a data breach a month earlier. *Id.* As a result of this incident, individuals whose PII was revealed in the data breach initiated a class action lawsuit against Victim-3.[6] *Id.* Victim-3 also describes incurring "substantial costs in the form of data breach response and remediation, security controls and improvements, business interruption, and the continued costs of litigation."[7] *Id.*

The activity on BreachForums also targeted the PII of ordinary Americans held by governmental entities. For instance, the Official CDN, which Fitzpatrick personally managed, uploaded a user database of the online training database for the Washington State Food Worker Course. *See* PSR at 42. The data trafficked on BreachForums included the user account information for approximately 1.5 million individuals, including name, date of birth, email

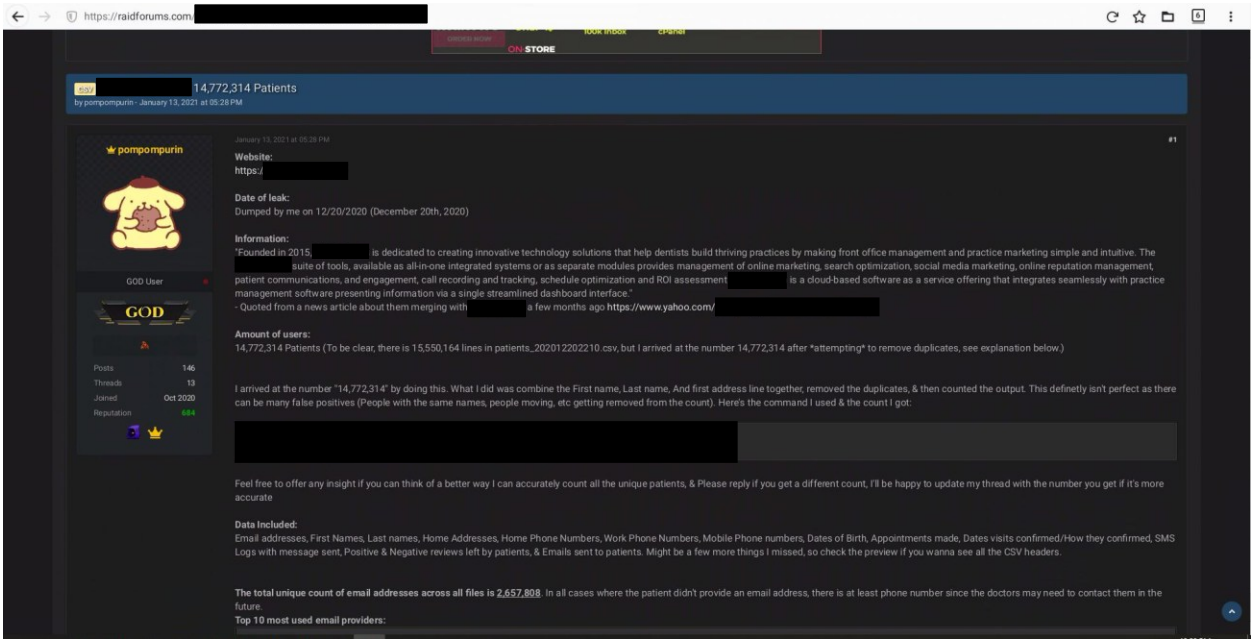
[5] The government notes that harm to reputation is not a pecuniary harm under §2B1.1.

[6] Victim-3 added the defendant as a third-party defendant to the civil litigation and in 2025, the defendant agreed to forfeit $700,000 to settle the civil lawsuit. *See* "Breachforums Boss to Pay $700k in Healthcare Breach" May 15, 2025 (available at: krebsonsecurity.com/2025/05/breachforums-boss-to-pay-700k-in-healthcare-breach/).

[7] After the first sentencing, Victim-3 withdrew its restitution request.

address, and zip code, and the driver's license numbers of approximately 9,500 individuals. *See id.*; *see also* Tacoma-Pierce County Health Department, "Data breach exposed Food Worker Card records. We are notifying those affected," *available at* https://www.tpchd.org/Home/Components/News/News/356/286 (July 6, 2023). The Tacoma-Pierce County Health Department reports that the discovery of the breach and associated trafficking of the data on the Official CDN consumed enormous amounts of public resources, including (i) approximately 607 hours of staff time investigating the breach, (ii) approximately 208 hours of staff time responding to emails, phone calls, and public records request, and (iii) approximately 45 hours of communications staff time drafting public notifications, preparing public documentation, sending notifications to 1.5 million email addresses, and responding to the media and the Tacoma-Pierce County Board of Health. *See* PSR at 42. This is time that the staff of the Tacoma-Pierce County Health Department could have spent serving their actual mission—protecting the public health of the county.

The defendant's criminal conduct also caused immense harm to Victim-5, a company offering software platforms for medical practices. *See* Exhibit 1. As depicted in the screenshot below, on or about January 13, 2021, the defendant, using his online moniker pompompurin, posted an announcement on Raidforums advertising a database dump of 14,772,314 patients' PII that had been downloaded from servers belonging to Victim-5.

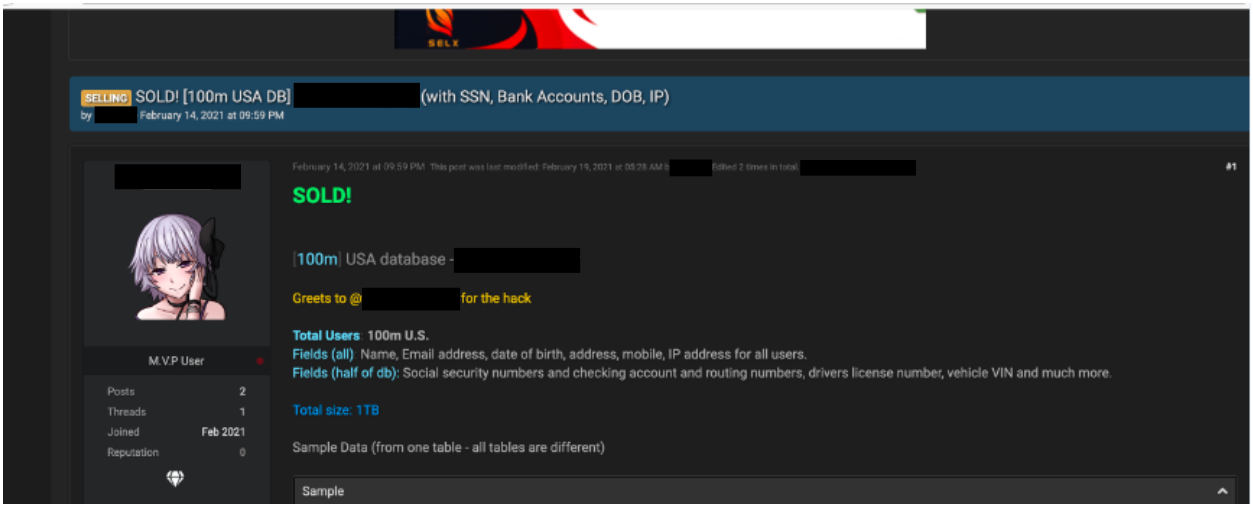



Victim-5 notified affected clients of the breach and informed them about the nature of the data that had been stolen. *Id.* at 1. "This disruption led to the issuance of credits and refunds for downtime equal to 31% of the company's 2020 revenue, the loss of several accounts, and damage to existing business relationships." *Id*. at 2. Victim-5's largest client requested concessions of more than $84,000. *Id*. Then, to make matters worse, in October 2021, an individual using email address pomlovesyou[at]riseup.net, and purporting to be the actor behind the data breach, contacted an employee of Victim-5 via email. *See id; id*. at 10 (email from pomlovesyou[at]riseup.net). The email contained abusive and harassing language, and threatened that the author would "take it upon [himself] to notify all of the businesses that got breached, LOL[.]" *Id*. He closed the email saying, "I hope you guys hang yourselves." *Id*. The following day, the individual emailed at least one of Victim-5's clients. *Id*.

Within a year of the data breach in December 2020, Victim-5, "which had been growing steadily, faced a significant decline in revenue, an inability to secure funding to turn the company around on its own, and the loss of a promising partnership and acquisition. This negative outlook

contributed to the most devastating consequence of all—the untimely death of [Victim-5's] founder and CEO [] who took his own life in November 2021 at the age of 54." *Id.* The CEO hanged himself in his home. *Id.* Victim-5 noted that the CEO had "leveraged a significant portion of his personal finances in the business and had obtained investments from friends and family, believing that the company would achieve the success that seemed likely before the attack." *Id.* at 2-3. Instead, Victim-5 was declared insolvent, and the company now expects to be merged into another company "for less than the value of the assets and software [they] built over the last ten years." *Id.* at 3.

Victim-4 is an advertising/marketing company based in the U.S. In 2021, Victim-4's server was hacked, and stolen company data was later advertised on RaidForums. *See* screenshot below.




The data was subsequently posted for sale on BreachForums in its Official CDN. The data was advertised as the names, email addresses, dates of birth, social security numbers, and checking

accounts for 100 million U.S. customers. According to Victim-4, the crimes have resulted in serious personal harm to the CEO and economic losses to the company.[8] *See* Exhibit 5.

In addition to the harm the defendant inflicted directly on his victims, he also personally served as the middleman for another BreachForums member who, without authorization, sold to an FBI OCE access to the accounting system of Victim-2, another healthcare company, and sample PII stored therein. PSR ¶¶ 48-52 and p. 35-37. Although the FBI's involvement mitigated the harm, Victim-2 reports that the incident still forced three senior engineers to spend approximately 63 hours investigating the breach and ultimately led it to detect unauthorized access from a foreign country. *Id.*

While the sheer volume of criminal activity on BreachForums, the victim impact statements, and the $698,714 of gain attributed to the defendant and his co-conspirators, underscore the seriousness of the defendant's crimes, the parties' stipulated gain enhancement reflects a highly conservative projection of the actual harm that the defendant caused. Indeed, this case presented a number of unique investigative challenges associated with quantifying the harm caused by the defendant's administration of BreachForums; particularly for the many millions of ordinary individuals whose PII was trafficked across the platform and then misused by unidentified

[8] The government requested additional information from Victim-4 to support its restitution claim, but as of this filing no additional information has been received. Many of the harms discussed by Victim-4, while extremely serious, are not clearly compensable under 18 U.S.C. § 3663A.

BreachForums members to facilitate financial fraud schemes.[9] Indeed, the FBI's annual "Internet Crime Report" for 2022 indicates that approximately $742,438,136 of the $1,201,759,995 reported damages from data breaches in 2022 were suffered by ordinary individuals whose personal data was released into an unsecure environment—*e.g.*, places like BreachForums. *See* FBI Internet Crime Report (2022), at 22, *available at* https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf. Further, in a recent report titled "Cost of a Data Breach: 2023," IBM Security reports that data breaches cost the average organization approximately $4.5 million and that customer PII, such as social security numbers, ultimately cost the organization approximately $183 per record. *See* Dkt. 65-4 (IBM Security, Cost of a Data Breach: 2023), at 9, 10, 18.

The defendant's possession of approximately 26 digital files depicting minors engaged in sexually explicit conduct, including two prepubescent minors, is also extremely serious. "It is well established that children featured in child pornography are harmed by the continuing dissemination and possession of that pornography. Such images are 'a permanent record of the children's participation and the harm to the child is exacerbated by their circulation.'" *United States v. Burgess*, 684 F.3d 445, 459 (4th Cir. 2012) (quoting *New York v. Ferber*, 458 U.S. 747, 759 (1982)); *accord United States v. Accardi*, 669 F.3d 340, 345 (D.C. Cir. 2012) ("[C]hild pornography creates an indelible record of the children's participation in a traumatizing activity, and the harm to the child is only exacerbated by the circulation of the materials."). "Every instance

[9] Calculating a precise loss figure is also challenging here because (i) of the diverse array of PII that was sold, offered, and trafficked on the platform, and (ii) many of the customer databases trafficked through the BreachForums Marketplace were not visible to law enforcement. In addition, some victim businesses and organizations have struggled to quantify how the significant negative publicity and regulatory attention caused by the posting of their user databases on BreachForums ultimately impacted their existing business relationships and ability to attract new customers, future investment, and new employees to their organizations.

of viewing images of child pornography represents a renewed violation of the privacy of the victims and a repetition of their abuse." Adam Walsh Child Protection and Safety Act of 2006, Pub. L. No. 109-248, § 501(2)(D), 120 Stat. 587, 624 (2006); *accord United States v. Sherman*, 268 F.3d 539, 547 (7th Cir. 2001) (recognizing that "[t]he possession, receipt and shipping of child pornography directly victimizes the children portrayed by violating their right to privacy, and in particular violating their individual interest in avoiding the disclosure of personal matters"). These children "must live with the knowledge that adults like [the defendant] can pull out a picture or watch a video that has recorded the abuse of [them] at any time," and they "suffer a direct and primary emotional harm when another person possesses, receives or distributes the material." *Sherman*, 268 F.3d at 547-48.

Here, through his possession of images and videos of child sexual abuse, the defendant perpetuated the victimization of the children whose exploitation is memorialized in those graphic depictions of their abuse. *See United States v. Daniels*, 541 F.3d 915, 924 (9th Cir.2008) (explaining that "merely possessing child pornography is not a victimless crime; it fuels the demand for the creation and distribution of child pornography").

For his crimes, the defendant has demonstrated little remorse; he violated the conditions of his pretrial release; he broke his cooperation agreement; and he denied responsibility for his child pornography offense. In his letter to the Court and at his first sentencing, the defendant nominally took responsibility for his crimes, but then blamed the people around him for his offenses. *See* Dkt. 69-1 (Defendant's letter to the Court) ("My intentions when creating the website were never to profit or make money, but to please the people that I talked to daily at that time."). In reality, the defendant rallied other cybercriminals to the cybercriminal forum that he created and administered. And he profited from his administration of BreachForums and from acting as the

middleman for criminal transactions. He shaped the cybercriminal landscape, not the other way around. And his lack of true remorse weighs in favor of a 188-month sentence.

**B. The History and Characteristics of the Defendant**

The defendant's criminal acts were not the product of a momentary lapse of judgement. Rather, for more than a year, the defendant made countless decisions as part of a brazen effort to create and lead the largest English-language data breach forum in the world. *See* PSR ¶¶ 35, 118-119 (indicating that he has never been employed and was not in school after May 2022). The defendant made these choices despite knowing that his conduct was illegal. Indeed, the defendant only elected to create BreachForums in March 2022 after law enforcement had taken down Raidforums and arrested the Raidforums founder in early 2022 on similar access device charges. *Id.* ¶¶ 18, 25, 26. For the defendant, the creation of BreachForums reflected a willful and defiant escalation of the types of criminal activity that he began pursuing as a prolific distributor of data breaches on Raidforums in 2020. *Id.* As previously detailed, the defendant's statements to other BreachForums members, use of fictitious identities to register many of BreachForums' domains, and reliance on online aliases to obscure his control over the platform, further highlight the willfulness of his crimes. *Id*. ¶¶ 26, 37, 53-55.

In addition, as previously detailed, the defendant engaged in a sustained pattern of violations of his bond conditions even after entering a guilty plea in this case. The defendant's use of one or more unmonitored devices and obfuscation services is particularly concerning given his history of committing cybercrime through false identities and anonymizing technology. *See also* Dkt. 65-1 (discussing history and characteristics of defendant).

Accordingly, although the defendant has no formal criminal history, the government believes the defendant's history of willful defiance of the law and malicious online activity

suggests a likelihood of recidivism if left undeterred by a significant term of incarceration. The risk of recidivism is particularly acute here given the defendant's repeated decisions to choose cybercrime over legitimate pursuits despite having opportunities that were never within the reach of many offenders who come before this Court, including a stable upbringing, financial support from his parents, educational opportunities, and impressive technical skills.[10]

The defense has argued that the defendant's ASD and other mental health challenges "explains (rather than excuses) how and why Conor will stand before the Court for sentencing." Dkt. 69 at 3. While the defendant's mental health diagnoses merit the Court's consideration, they do not warrant a variance from the Guidelines. Notwithstanding the defendant's diagnosis, he managed to establish a full-fledged online universe devoted to facilitating cybercrime across the globe. The defendant carefully choreographed BreachForums to allow its hundreds of thousands of users to maximize their illegal activity and trade in confidence. The defendant designed and administered the site's software and computer infrastructure. He kept the site running through the purchase of multiple domain names, employed and managed a paid staff to help administer the site, established a credit system, created and implemented processes for buying and selling hacked or stolen information, enforced the site's rules, and encouraged users to spread the word when sharing databases.

Notwithstanding the communication and social challenges posed by the defendant's autism, he managed to broker hundreds of thousands of dollars' worth of deals through his middleman service. There is also no question that the defendant knew what he was doing was

[10] "Criminals who have the education and training that enables people to make a decent living without resorting to a crime are more rather than less culpable than their desperately poor and deprived brethren in crime." *United States v. Stefonek*, 179 F.3d 1030, 1039 (7th Cir. 1999).

wrong. He even helped one BreachForums member who feared law enforcement scrutiny delete his or her IP address from the site. He promised another user that he would falsify registration information should law enforcement ever request it, jokingly stating that he "doubt[ed] law enforcement would even bother making legal requests to a hacking forum lmao[.]" And in brokering a deal between the OCE and "expo2020" for the PII of 15 million U.S. persons, the defendant only released the payment after the OCE confirmed he would use the PII to commit financial crimes.

Fundamentally, the defendant's mental health conditions have little bearing on his criminal conduct and are simply not sufficiently compelling to warrant a variance from the Guidelines. At his first sentencing, the defendant argued he had "never been given an opportunity to have proper treatment, to have proper attention, and somebody really monitoring him." Dkt. 77 at 17. In fact, the defendant had been seeing a therapist for several years before he was charged with the instant offenses. He received inpatient treatment for two weeks in November 2019 and then weekly individual counseling until April 2023. PSR ¶ 114. From April 2023 until May 17, 2023, he received in-patient treatment. *Id*. ¶ 115. When he was released from in-patient treatment, he attended virtual group sessions three times per week and weekly individual sessions until August 2023. *Id*. In September 2023, the defendant moved to weekly individual sessions, which continued until his incarceration. *Id*., *see also* Dkt. 77. at 21 (The defendant stated, "I've also been working on my mental health by going to therapy two times a week, taking evaluations, and being open fully to any treatments that would better myself."). The defendant was meeting with a therapist on a weekly basis while he was violating his pretrial release conditions. In other words, the defendant has had treatment for many years, and yet he continued to engage in criminal conduct.

While the government does not dispute the defendant's ASD diagnosis, it is important to note that the defendant's ASD is mild and there is no reason to believe that he cannot cope in a prison setting. In April 2025, the defendant was evaluated by Dr. Darrel Turner, a licensed psychologist and former BOP Staff Psychologist, who concluded that the defendant's overall "degree of impairment [] due to his ASD is low." *See* Exhibit 2 (Dr. Turner Report) at 7; Exhibit 3 (Dr. Turner CV). Dr. Turner noted that while the defendant may struggle with social interactions, he "is not averse to social interaction"—a conclusion supported by the defendant's discussion of going into New York City on the weekends with his friends, for example. *Id*. Dr. Turner also noted the defendant "completed his schooling successfully without accommodation for any impairment and attended a community college for a time, also without accommodation." *Id*. Dr. Turner observed that the defendant's desire to eventually "start a family and live outside of his parents' home and secure a job and career speak positively to his ability to cope with his symptomology in a healthy manner." *Id*. "When asked what accommodations he felt would benefit him," the defendant stated, "maybe a private room and extra time." *Id*. Dr. Turner noted that "[i]f the overall impairment caused by the disorder is on the milder end" – as he concluded the defendant's is – "individuals can learn to tolerate less pleasant stimuli more effectively." *Id*.

Dr. Turner reviewed the programming and treatment options supplied by BOP in this case. *See* Exhibit 4 (BOP Memorandum). Dr. Turner attested to BOP's care and treatment of inmates with mental health diagnoses, noting that "[a]s a previous employee of the Federal Bureau of Prisons as a staff psychologist, [he] conducted these intake evaluations for years. Every new inmate is seen by multiple mental health experts – some mandated to be at the doctoral level – and their mental health needs and concerns are individually addressed." Exhibit 2 at 11. Further, "[t]hese clinical encounters, in conjunction with a review of available mental health data . . . and

other historical and dynamic factors, are considered in the assignment of Mr. Fitzpatrick to a specific CARE level for medical and mental health purposes." *Id.* Dr. Turner noted that inmates "are well cared for and integrate effectively into the prison community based on the structure of the care they receive." *Id.* Further, "[t]here are psychologists whose career track in the BOP is based solely on providing care for and supervising care for these individuals." *Id.*

Based on his evaluation and review of the defendant's prior psychological evaluations, Dr. Turner concluded that the defendant "will be able to cope with and function in the Federal Prison System with an appropriate level of care specifically tailored for his needs." Exhibit 2 at 11. Further, "the overall level of impairment caused by Mr. Fitzpatrick's autism spectrum disorder is mild and, as he has shown, he is improving in therapy and across time and will likely continue to do so as long as he is engaged in his own well-being and self-improvement." *Id*. at 10-11.

The BOP has made significant effort to meet the needs of inmates struggling with mental health issues. Indeed, BOP is now required by law to implement "specialized and comprehensive" training in procedures to "identify and appropriately respond to incidents that involve the unique needs of individuals who have a mental illness or cognitive deficit." *See* First Step Act of 2018, Pub. L. No. 115-391, § 606, 132 Stat. 5194, 5244.17. The First Step Act requires the BOP to create a "risk and needs assessment system." *See* First Step Act of 2018, Pub. L. No. 115-391, § 101, 132 Stat. 5194, 5195.

Upon arrival, "newly incarcerated individuals undergo a mental health intake screening with a doctoral level psychologist to identify treatment needs and determine if the individual would benefit from referral to a specific treatment program." Exhibit 4 (BOP Memorandum) at 2. "A mental health care level (1 through 4) is assigned to the inmate based on the inmate's needs." *Id.* Whether the inmate is level 1 or level 4, they can request mental health services. *Id.* Furthermore,

"[a]ll institution psychologists are trained on conducting suicide risk assessments and can offer a variety of psychology programming such as Brief Cognitive Behavioral Therapy for suicidal inmates, DBT Skills Training, and Mindfulness Based Cognitive."[11] Notably, "[i]ndividual and group therapy can be offered at any facility" and according to BOP "would likely address symptoms discussed in the evaluations for [the defendant]." *Id*. Inmates convicted of sex offenses are offered sex offender treatment at a Sex Offender Management Program (SOMP) facility, with a large number of inmates presenting issues similar to the defendant's. *Id*.

In addition to sex offender treatment, BOP offers the Skills Program, which is "designed for inmates with significant cognitive limitations and psychological difficulties that create adaptive problems in prison and in the community." [12] The Skills Program "uses an integrative model which includes a modified therapeutic community, cognitive-behavioral therapies, and skills training."[13] "The goal of the program is to increase the academic achievement and adaptive behavior of cognitively impaired inmates, thereby improving their institutional adjustment and likelihood for successful community reentry." *Id*. The Skills Program "employs a multi-disciplinary treatment approach aimed at teaching participants basic educational and social skills." *Id.* The program addresses criminal thinking "through the identification of criminal thinking errors

[11] According to his May 2023 psychiatric evaluation, the defendant was recommended to engage in dialectical behavior therapy (DBT) (*see* PSR ⁋ 115), which is offered at any BOP facility (Exhibit 4 at 2).

[12] *See* "Psychology Treatment Programs" at 62, dated April 25, 2016 (available at: www.bop.gov/policy/progstat/5330.11.pdf); First Step Act Approved Programs Guide, available at: www.bop.gov/inmates/fsa/docs/fsa_guide_eng_2023.pdf (September 2023); "Management of Inmates with Disabilities" at 6, dated November 22, 2019 (available at: www.bop.gov/policy/progstat/5200_06.pdf).

[13] *See* "Directory of National Programs" at 20 (available at: www.bop.gov/inmates/custody_and_care/docs/20170518_BOPNationalProgramCatalog.pdf).

and engagement in prosocial interactions with staff and peers." *Id*. Ultimately, the program "content is designed to promote successful reentry into society at the conclusion of their term of incarceration." *Id*. The BOP's Psychology Services Branch Administrator and its Acting Assistant Director of Reentry Services reviewed the defendant's PSR and prior psychological evaluations and concluded that if sentenced to BOP custody, "[the defendant's] mental health needs and programming will be fully explored to ensure he is offered the services necessary." *See* Exhibit 4 at 3.

The concerns raised in the defendant's prior psychological evaluations (*see* PSR ¶ 115; Dkt. 69-2; Dkt. 69-3) do not warrant a variance from the Guidelines, and as stated above, are allayed by the many treatment options available in BOP and the defendant's mild ASD diagnosis. Furthermore, the defendant's mental health evaluations do not opine that he is categorically unfit for prison or that BOP could not provide the type of care recommended by the evaluators. Rather, they raised three primary concerns related to his incarceration (Dkt. No. 69-2 at 11), none of which justifies a variant sentence.

*First*, Dr. Belchic Schwartz noted that individuals with ASD may struggle with communication, leading to misunderstandings in prison and possibly disciplinary issues. *Id*. Accordingly, per Dr. Belchic Schwartz, the defendant "faces an increased risk of victimization." *Id*. Critically, the report offered no further analysis regarding possible victimization and whether that would be physical harm or, as the evaluator noted, the harm that could stem from the defendant being unable to fully advocate for himself. Further, the evaluation never addressed why BOP would not be equipped to manage the defendant's "increased risk of victimization." *Id*.

*Second*, Dr. Belchic Schwartz noted that individuals with ASD have heightened sensitivity to sensory stimuli, which can be exacerbated in a prison environment. Dkt. No. 69-2 at 11.

However, there is no evidence that the defendant personally suffers from any sensory stimuli issues. Consequently, this general concern about individuals who suffer from increased sensory sensitivities may not even apply to the defendant. Though even if it did, Dr. Turner noted that because the defendant's ASD is on the "milder end," he will be able to learn to tolerate less pleasant stimuli more effectively.

*Third*, Dr. Belchic Schwartz noted that people with ASD often thrive in structured and predictable environments. *Id*. And the "dynamic and unpredictable nature of prison life may lead to increased stress for [the defendant], impacting his mental health and wellbeing." *Id*. The last point is particularly hard to understand, as it is difficult to imagine a setting that is *more* structured and predictable than prison.

In recognition of the defendant's age and medical background, the government proposes a sentence of 188 months that is at the low end of the Guidelines. However, in view of the seriousness of the defendant's sustained and willful conduct, the defendant's history and characteristics do not merit any further variance or departure and support a significant sentence. There is no evidence that the defendant's ASD caused his criminal conduct or caused him to not fully understand the harmfulness or illegality of his conduct. The defendant knew what he was doing was harmful and illegal and chose to do it anyway.

### C. The Sentence Should Deter Leaders of Organized Cybercrime

According to the Internet Crime Report for 2022, the FBI received reports of 58,859 personal data breaches and 2,795 organizational data breaches that caused complained total losses of approximately $1,201,759,995 in 2022 alone. *See* FBI Internet Crime Report (2022), at 22 and 24. The IBM "Cost of a Data Breach Report" for 2023 estimate that U.S. organizations suffered data breach losses of approximately $9.48 billion. Dkt. 65-4 at 11.

To deter and disrupt cybercriminals who would seek to profit from data breaches, it is critically important to punish the leaders of the cybercrime ecosystem. In recent years, judges in this District have considered, at sentencing, the widespread harm that leaders and organizers of cybercrime inflict. *See, e.g., United States v. Bondars et al.*, 1:16-cr-228-LO (E.D. Va.), Dkt. 233, at 23–26 (sentencing transcript containing Court's observation that defendant who created and operated a tool "facilitating, aiding and abetting enormous numbers of hackers" needed to be deterred and that seriousness of crimes warranted 168-month sentence); *United States v. Burkov*, 1:15-cr-245-TSE (sentencing defendant to nine years in prison for his operation of two cybercrime websites that resulted in over $20 million in fraudulent purchases); *United States v. Tverdokhlebov* 1:17-cr-9 (E.D. Va.) (110 months for defendant who sold and trafficked sensitive personal and financial information on cybercrime forums). Likewise, defendants convicted in other districts of running online marketplaces that facilitated hacking or various forms of identity and access device theft have received significant sentences. *See e.g., United States v. Pakhtusov*, 1:19-cr-310 (D.D.C.) (61 months for cooperating defendant who sold access devices on cybercrime forums); *United States v. Diaconu*, 8:20-cr-238 (M.D. Fla.) (42 months for defendant who operated website that sold access to compromised computer servers). None of these defendants had the additional child pornography conviction present in this case.

Here, the defendant incentivized and turbocharged the marketplace for data breaches by operating BreachForums in a manner designed to help cybercriminals overcome the "skill, trust, and funding barriers which inhibit the development of truly mass-scale cybercrime economies" and helped buyers "find sellers in scam-ridden underground communities." Collier, Cybercrime Economies, at 5. A significant sentence is needed to deter a future wave of leaders of the cybercrime ecosystem.

Further, as this case illustrates, cybercriminals exploit the invisibility afforded by the Internet, cryptocurrency, and other masking tools to evade detection for many years and earn significant rewards. Indeed, many Internet crimes go unsolved and unpunished due to the tremendous resources it takes for law enforcement to pierce through a cybercriminal's cloak of anonymity. As the Honorable J. Harvie Wilkinson, III observed in an access device prosecution:

> Financial fraud is a modern scourge. It preys especially upon the unsophisticated and vulnerable. As the district court noted, crimes like those in this case harm victims 'in almost irreparable ways by causing them loss of work, mental anguish, monetary loss, and loss of peace of mind.' J.A. 152. It raises costs for businesses, which must invest in security measures. These crimes require time and expertise to investigate and can be difficult to unravel and prove.

*United States v. Carver*, 916 F.3d 398, 404 (4th Cir. 2019).

Accordingly, when a sophisticated cybercriminal like the defendant is identified and apprehended, a substantial sentence is needed to deter others from pursuing the same path. *See United States v. Hayes*, 762 F.3d 1300, 1308 (11th Cir. 2012) ("[G]eneral deterrence is an important factor in white-collar cases, where the motivation is greed."); *United States v. Martin*, 455 F.3d 1227, 1240 (11th Cir. 2006) (Because "economic and fraud-based crime are more rational, cool, and calculated than sudden crimes of passion or opportunity, these crimes are prime candidates for general deterrence" (internal quotations and citation omitted)).

**D. Supervised Release**

The Court must also determine the appropriate term of supervised release at sentencing. "Supervised release . . . is not a punishment in lieu of incarceration." *United States v. Granderson*, 511 U.S. 39, 50 (1994). Instead, it "fulfills rehabilitative ends, distinct from those served by incarceration." *United States v. Johnson*, 529 U.S. 53, 59 (2000). Under 18 U.S.C. § 3583(b)(2), the authorized term of supervised release for Counts 1 and 2 is not more than 3 years, and under

Section 3583(k), the authorized term for Count 3 is at least five years and up to life. This five-year mandatory minimum term for Count 3 reflects a heightened concern for recidivism among sex offenders and the need for supervision over time. *See, e.g.*, H.R. Rep. No. 107-527, at 2 (2002) (explaining that "studies have shown that sex offenders are four times more likely than other violent criminals to recommit their crimes" and that "the recidivism rates do not appreciably decline as offenders age"). Notably, the Guidelines recommend a lifetime term of supervised release for sex offenders, USSG § 5D1.2(b) (Policy Statement), and the Fourth Circuit has observed that § 3583(k) and § 5D1.2(b) jointly "reflect[] the judgment of Congress and the Sentencing Commission that a lifetime term of supervised release is appropriate for sex offenders in order to protect the public." *Morace*, 594 F.3d at 351 (citations omitted).

The defendant's conduct—namely, his years-long use and subsequent administration of online cybercrime forums, his attempts to evade law enforcement detection, and his pretrial violation and associated failure to clearly demonstrate acceptance of responsibility for his crimes—underscores the need for a substantial term of supervised release to ensure the defendant is properly monitored and can access rehabilitation services. For these reasons, the United States respectfully recommends that the Court impose a substantial term of supervised release with the conditions of supervision contemplated under 18 U.S.C. § 3583(d) and USSG § 5D1.3(d)(7) for sex offenders required to register under the Sex Offender Registration and Notification Act.

### E. Special Assessments Under the Justice for Victims of Trafficking Act (JVTA) & the Amy, Vicky, and Andy Child Pornography Victim Assistance Act (AVAA)

On December 7, 2018, Congress enacted the Amy, Vicky, and Andy Child Pornography Victim Assistance Act. The Act instructs that, in addition to any restitution or other special assessment, courts "shall assess . . . not more than $17,000 on any person convicted of an offense

under section 2252(a)(4) . . . ." 18 U.S.C. §§ 2259A(a)(1). Assessments collected under this statute are deposited in the Child Pornography Victims Reserve, which provides monetary assistance to victims of trafficking in child pornography, *see* §§ 2259(d) & 2259B, and shall be paid in full after any special assessment under § 3013 and any restitution to victims of the defendant's offense, *see* § 2259A(d)(2). In determining the amount to be assessed under § 2259A, courts should consider the sentencing factors set forth in § 3553(a) and the guidance in § 3572 for the imposition of fines. § 2259A(c). The United States respectfully requests that the Court impose a reasonable special assessment under § 2259A, in addition to the $300 mandatory special assessment for the defendant's felony convictions pursuant to 18 U.S.C. § 3013.

Additionally, under the Justice for Victims of Trafficking Act, courts "shall assess an amount of $5,000 on any non-indigent person" convicted of certain enumerated offenses, including possession of child pornography. *See* 18 U.S.C. § 3014. The United States respectfully requests that the Court impose an assessment of $5,000 for the defendant's convictions pursuant to 18 U.S.C. § 3014.

**F. Restitution**

As part of the plea agreement entered into by the parties, and pursuant to 18 U.S.C. § 3663A(c)(1) and (c)(2), the defendant has agreed to entry of a Restitution Order for the full amount of the victims' losses as determined by the Court. Upon information and belief, the defendant has agreed to pay restitution to Victim-1 in the amount of $183,284.30 and Victim-2 in the amount of $3,798. Victim-3 withdrew its restitution request.

Since this case was set for resentencing, the government received an additional restitution request from Victim-5, which was provided to defense counsel and Probation. The government requests the Court order the defendant to pay restitution to Victim-5 in the amount of $829,704.21.

The Mandatory Victim Restitution Act of 1996 (the MVRA) requires courts to order that defendants convicted of covered crimes pay restitution to the victims of those crimes. 18 U.S.C. § 3663A(a)(1). The act applies to "offense[s] against property under [Title 18] . . . including any offense committed by fraud or deceit" in which "an identifiable victim or victims has suffered a . . . pecuniary loss." *Id.* § 3663A(c)(1)(A)(ii) & (B). The term victim means any "person directly and proximately harmed as a result of the commission of an offense for which restitution may be ordered." *Id.* § 3663A(a)(2). "When the crime involves a scheme or pattern of criminal activity, the universe of victims includes 'any person directly harmed by the defendant's criminal conduct in the course of the scheme, conspiracy, or pattern.' " *United States v. Lomas*, 392 F. App'x 122, 127 (4th Cir. 2010). Restitution should be awarded for the actual losses sustained by the victim. *United States v. Squirrel*, 588 F.3d 207, 213 (4th Cir. 2009). And the Court should impose restitution "without consideration of the economic circumstances of the defendant." 18 U.S.C. § 3663A(f)(1)(A).

The letter from Victim-5's CEO lays out the following compensable losses incurred by Victim-5 as a result of the defendant's criminal conduct:

- $226,704.21 in credits and rebates issued to clients impacted by the data breach; and
- $603,000 in cancelled contracts as a result of the data breach. *See* Exhibit 1 at 5.

The defendant's actions directly and proximately harmed Victim-5. He hacked and stole data from Victim-5's servers, including patient PII, and advertised it on RaidForums. The defendant also destroyed and damaged databases and data tables, requiring a significant amount of time and money to rebuild. *See* Exhibit 1 at 2. The $829,704.21 that the government is seeking for restitution to Victim-5 reflects actual losses to Victim-5 from the defendant's criminal conduct, namely issuing credits and rebates to affected clients and cancelling contracts with companies who

lost trust in Victim-5 as a result of the data being stolen and advertised online. The Court therefore should award restitution in this amount.

**G. Forfeiture**

The United States submitted a consent order for forfeiture, signed by the defendant and his counsel, during the plea agreement hearing. *See* Dkt. 42. The order was signed by the Court the same day. The government requests the Court reincorporate in its new Judgment the consent order of forfeiture previously entered.

## CONCLUSION

For the reasons above, the United States respectfully requests that the Court impose a sentence at the low end of the Guidelines, a substantial term of supervised release, a $300 special assessment under § 3013, a $5,000 special assessment under § 3014, a reasonable special assessment under § 2259A, and restitution in the amount of $1,016,786.51 to the victims.

Respectfully submitted,

Erik S. Siebert
United States Attorney

Date: September 8, 2025

By: /s/

Lauren Halper
Assistant United States Attorney
United States Attorney's Office
2100 Jamieson Avenue
Alexandria, Virginia 22314
Phone: (703) 299-3700
Fax: (703) 299-3980
Email: Lauren.Halper@usdoj.gov

AND

Thomas S. Dougherty
Senior Counsel
Computer Crime and Intellectual Property Section
U.S. Department of Justice, Criminal Division